AO-106 (Rev: 06/09)-Application for Search Warrant

FILED

APR 16 2024

Mark C. McCartt, Clerk
U.S. DISTRICT COURT

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
an Apple iPhone A177; Samsung SM-G970u; Samsung SGH-I337; Samsung SM-G891A IMEI 358518072719411; Samsung SM-G850A; Samsung SM-G930A; 7 thumb drives; 5 SD Cards; SanDisk Ultra Plus 32 GB; SanDisk Extreme Pro 32 GB; Western Digital External Hard Drive; Seagate External Hard Drive; 16 GB SanDisk card; Apple iPad 4; ACER Laptop; HP Laptop; Alienware Aurora; and a Dell Laptop Currently Stored at the Homeland Security Investigations Tulsa Office

Case No. 24-mj-284-SH

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2252(a)(2) and (b)(1)	Receipt and Distribution of Child Pornography
18 U.S.C. §§ 2252(a)(4)(A) and (b)(2)	Possession of Child Pornography in Indian Country

The application is based on these facts:

See Affidavit of SA Erin Staniech, HSI, attached hereto.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Erin Staniech, Special Agent HSI
Printed name and title

Subscribed and sworn to by phone.

Date: 4/16/24

Judge's signature

City and state: Tulsa, Oklahoma

Susan E. Huntsman, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF OKLAHOMA

In the Matter of the Search of an Apple iPhone A177; Samsung SM-G970u; Samsung SGH-I337; Samsung SM-G891A IMEI 358518072719411; Samsung SM-G850A; Samsung SM-G930A; 7 thumb drives; 5 SD Cards; SanDisk Ultra Plus 32 GB; SanDisk Extreme Pro 32 GB; Western Digital External Hard Drive; Seagate External Hard Drive; 16 GB SanDisk card; Apple iPad 4; ACER Laptop; HP Laptop; Alienware Aurora; and a Dell Laptop Currently Stored at the Homeland Security Investigations Tulsa Office	**Case No.** _____

Affidavit in Support of an Application
Under Rule 41 for a Warrant to Search and Seize

I, Erin Staniech being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession,

and the extraction from that property of electronically stored information described in Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant.

3. I have been employed as a Special Agent ("SA") with Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI") since June 2019. I am currently assigned to the Office of the Resident Agent in Charge in Tulsa, Oklahoma, and am currently assigned to investigate crimes involving child exploitation. While employed by HSI, I have investigated federal criminal violations related to child exploitation and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center's (FLETC) twelve-week Criminal Investigator Training Program (CITP) and the sixteen-week Homeland Security Investigations Special Agent Training (HSISAT) program, and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have received focused child exploitation training covering topics such as: interview techniques, live streaming investigations, undercover investigations, capturing digital evidence, transnational child sex offenders, and mobile messaging platforms utilized by these types of

offenders. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252(a), and I am authorized by law to request a search warrant.

4. As part of my duties as an HSI agent, I investigate criminal violations relating to child pornography, including the production, transportation, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. I have received training in the areas of child pornography and child exploitation and have observed and reviewed numerous examples of child pornography, as defined in 18 U.S.C. § 2256, in all forms of media. I have been involved in several child pornography investigations and am familiar with the tactics used by individuals who collect and distribute child pornographic material.

5. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

6. Based on my training, experience, and the facts set forth in this affidavit, there is probable cause to believe that evidence of violations of Title 18 U.S.C. §§

2252(a)(2) and (b)(1) (Receipt and Distribution of Child Pornography) and 18 U.S.C. §§ 2252(a)(4)(A) and (b)(2) (Possession of Child Pornography in Indian Country) will be located in the electronically stored information described in Attachment B and is recorded on the Devices described in Attachment A.

Jurisdiction

7. "[A] warrant may be issued to search for and seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States." 18 U.S.C. § 3103a.

8. The requested search is related to the following violations of federal law:

a. Title 18, United States Code, Sections 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction that has been mailed, shipped, or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct; and

b. Title 18, United States Code, Sections 2252(a)(4)(A) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by

computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

9. Venue is proper because the person or property described in this affidavit is located within the Northern District of Oklahoma. Fed. R. Crim. P. 41(b)(1).

Identification of the Device to be Examined

10. The following is a list of property, hereinafter the "Devices":

1. Apple iPhone A1778 IMEI 358586092672637;
2. Samsung SM-G970u IMEI 352811101068728;
3. Samsung SGH-I337 IMEI 356567057346213;
4. Samsung SM-G891A IMEI 358518072719411;
5. Samsung SM-G850A IMEI 355956060549569;
6. Samsung SM-G930A IMEI 357425077311619;
7. 7 thumb drives;
8. 5 SD Cards;
9. SanDisk Ultra Plus 32 GB;
10. SanDisk Extreme Pro 32 GB;
11. Western Digital External Hard Drive;
12. Seagate External Hard Drive;

13. 16 GB SanDisk card (found in a White Nikon Coolpix Camera);

14. Apple iPad 4;

15. ACER Laptop;

16. HP Laptop;

17. Alienware Aurora R5 GTX1070; and

18. Dell Laptop S/N 27807611078.

The Devices are currently located at 125 W 15th Street Tulsa, Oklahoma 74119.

11. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

Definitions

12. The following definitions, inclusive of all definitions contained in 18 U.S.C. § 2256, apply to this affidavit and the attachments incorporated herein:

a. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-

generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct;

b. "Internet Protocol address" or "IP address" refers to a unique number used by a computer or electronic device to access the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses may also be static, which means the ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet;

c. "Electronic Mail," commonly referred to as email (or e-mail), is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the Internet or other computer networks. Email systems are based on a store-and-forward model; that is, email servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need only connect briefly, typically to an email server, for as long a period of time as it takes to send or receive messages. One of the most commons methods of obtaining an email account is through a free web-based email service provider such as, Outlook, Yahoo, or Gmail. Anyone with access to the Internet can generally obtain a free web-based email account;

d. A "hash value" or "hash ID" is a unique alpha-numeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file's content. A hash value is a file's "digital fingerprint" or "digital DNA." Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names;

e. "MD5" is a specific type of hash value that serves as a digital fingerprint for a file. The National Center for Missing & Exploited Children uses MD5 when referring to hash values or IDs.

f. "Cloud storage service" refers to a publicly accessible, online storage provider that can be used to store and share files in large volumes. Users of cloud storage services can share links and associated passwords to their stored files with others in order to grant access to their file collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop computers, laptops, mobile phones or tablets, from anywhere. Many services provide free access up to a certain size limit;

g. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international

borders, even when the devices communicating with each other are in the same state;

h. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years;

i. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form;

j. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person; and

k."Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

l. An "Secure Digital Card" otherwise known as an "SD Card" is a flash memory card developed for use in portable devices. SD cards were developed and used primarily for storage in mobile electronics such as cameras and smart devices. SD cards can hold up to a certain amount of information. SD cards can

be removed from one device and placed in a different device if that device has a built in SD card reader, or if a media card reader that plugs into a USB port is used.

Peer-to-Peer File Sharing

13. One way of sharing files on the Internet is peer-to-peer file sharing ("P2P"). P2P is a method of communication available to Internet users through the use of special software. The software is designed to allow users to trade digital files through a worldwide network that is formed by linking computers together. There are several different software applications that can be used to access these networks, but these applications operate in essentially the same manner.

14. To access the P2P networks, a user first obtains the P2P software, which can be downloaded from the Internet. This software is used exclusively for the purpose of sharing digital files. Generally, when P2P software is installed on a computer, the user is directed to specify a "shared" folder. All files placed in that user's "shared" folder are available to anyone on the worldwide network for download. However, a user is not required by all programs to share files to utilize a P2P network.

15. A user obtains files by conducting keyword searches of the P2P network. When a user initially logs onto a P2P network, a list of the files that the user has designated for sharing is transmitted to the network. The P2P software then matches files in these file lists to keyword search requests from other users. A user looking to download files simply conducts a keyword search. The results of the keyword search are displayed and the user then selects a file or files which he or she wants to

download. The download of a file is achieved through a direct connection between the computer requesting the file and the computer or computers hosting the file. Once a file has been downloaded, it is stored in the area previously designated by the user and will remain there until moved or deleted. Most of the P2P software applications keep logs of each download event. Often a forensic examiner, using these logs, can determine the IP address from which a particular file was obtained.

16. A person interested in sharing child pornography with others in the P2P network need only place those files in his or her "shared" folders. Those child pornography files are then available to all users of the P2P network for download regardless of their physical location.

17. A person interested in obtaining child pornography can open the P2P application on his or her computer and conduct a keyword search for files using a term such as "preteen sex." The keyword search would return results of files being shared on the P2P network that match the term "preteen sex." The user can then select files from the search results and those selected files can be downloaded directly from the computer or computers sharing those files. However, some P2P networks allow users to preview image files in thumbnail view and the filenames of video files. Thumbnail view is a small image of the file which will appear larger if it is downloaded. The user can then select files from the previews and filenames and those files can be downloaded directly from the computer or computers sharing those files.

18. The computers that are linked together to form the P2P network are located

throughout the world; therefore, the P2P network operates in interstate and foreign commerce. A person that includes child pornography files in his or her "shared" folders is hosting child pornography and therefore is promoting, presenting, and potentially distributing child pornography. A person who hosts child pornography is in violation of Title 18, United States Code, Section 2252A(a)(3)(B) in that he or she is promoting and presenting child pornography in interstate and foreign commerce by means of a computer.

19. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a user downloading an image file may actually receive parts of the image from multiple computers.

20. On some P2P networks, a user can create two types of folders to share files with other individuals on his/her network: "read-write" folders and "read-only" folders. If a user creates a "read-write" folder, other individuals on his/her network may: (1) view the contents of the folder; (2) download the contents of the folder; and (3) upload files to that folder. If, on the other hand, the user creates a "read-only" folder, others on his/her network cannot upload files to the "read-only" folder, they can only view and download the contents of that folder. Thus, when child pornography is present in a "read-only" folder, it could only have been placed there by the creator of the folder or someone else with a username and password associated with that folder. No other user in the network can upload files to a "read-

only" folder.

21. On other P2P networks, the software is not designed to permit folders to be configured as "read-write." Therefore, one user cannot send or upload a file to a second user of these P2P networks without the second user's active participation. The software is designed only to allow files to be downloaded from the P2P network. One does not have the ability to send files from his/her computer to a second user's computer without the second user's permission or knowledge. Therefore, on some P2P networks one user cannot send or upload child pornography to a second user's computer without the active participation of the second user.

Probable Cause

22. In September 2019, Sapulpa Police Department (SPD) Lt. Mark Swafford began a peer-to-peer file sharing investigation involving the distribution of child pornography, herein referred to as child sexual abuse material (CSAM). While conducting the investigation, Lt. Swafford identified an IP address, 72.203.181.25, that had downloaded at least five files of what appeared to be CSAM material. These downloads were taking place on the peer-to-peer file sharing network called BitTorrent.

23. A subpoena was sent to Cox Communications, Inc., requesting subscriber information for the IP address 72.203.181.25. On November 8, 2019, Lt. Swafford received the subscriber information from Cox Communications Inc., which showed that the IP address was associated with a Joseph KOSS at 524 N. Ridgeway St., Sapulpa, Oklahoma 74066 with a telephone number of 918-810-8024.

24. Based off Lt. Swafford's investigation, a Creek County judge signed a State of Oklahoma search and seizure warrant on November 19, 2019 for the residence located at 524 N. Ridgeway St., Sapulpa, Oklahoma 74066.

25. The State of Oklahoma search and seizure warrant was executed on November 22, 2019. Joseph KOSS was located at the residence and items 1-18 were seized from the residence pursuant to the search warrant.

26. KOSS was interviewed at the scene by Lt. Swafford and Tulsa Police Department Detective Rob McCoy. Detective McCoy told KOSS that he was not under arrest and that he was free to leave at any time during the interview. According to Lt. Swafford's report, KOSS made the following statements during the interview:

a. That he lives at the residence with his wife Ruth Patrick Koss.
b. That he worked for the Oklahoma Department of Human Services (OKDHS) and investigated child abuse and neglect allegations.
c. That he has two cell phones, one of which is owned by the state of Oklahoma and used for his job.
d. That his personal cellphone is a Samsung.
e. That he has a laptop computer that he does not use much.
f. That the Alien computer was used for gaming and he purchased it from BestBuy.
g. That he has a password protected Wi-Fi system at his residence.

h. That his cellphone is password protected and the passcode is 0211.

i. That the passcode for the iPad is also 0211.

j. That the passcode to the desktop computer is Allendale1.

k. That the only people to have access to the desktop computer are he and his wife.

l. That people have come to his house and used his computer before but that has not occurred in approximately 6 months.

m. That he is unaware of any computer viruses including Trojan Horse or unauthorized remote in access.

n. That he used BitTorrent program a long time ago.

o. That he is familiar with the BitTorrent program and that he was able to explain that it is a file sharing program that allows people to have files on their computer and share those files with other people. Koss stated that he knows how to use the program and admitted that there "might be" a BitTorrent program on the desktop computer.

p. That he might have seen CSAM while working in law enforcement but that it is junk and he does not look at it.

q. That he does not look at any pornography.

r. That he, for the most part, was responsible for the data stored on the desktop, laptop, iPad, and both cellphones.

s. That his wife is not the individual downloading CSAM.

t. That he was accused of inappropriately touching a 4 year old child during a OKDHS investigation to which he was assigned. The child was forensically interviewed and did not disclose any abuse.

u. That he believed the family who made the accusation was tired of being harassed by OKDHS and he was the unfortunate one.

v. That people convicted of possessing CSAM should go to prison, throw them underneath the prison and throw away the key.

w. That there is no excuse for downloading/possessing CSAM and the demand for it would not be there is there were not people to consume it.

27. KOSS was given the opportunity to leave the scene after questioning; however, he chose to sit in a chair in the living room.

28. KOSS's wife was not present when the search warrant was conducted at her residence. She was interviewed later that same day at the Glenpool Police Department by Lt. Swafford and Detective McCoy. Her electronic devices were on her person at the time of the interview and her devices were not taken from her by law enforcement. According to Lt. Swafford's report, KOSS's wife made the following statements:

a. That she has never downloaded CSAM and has never seen CSAM on the home computer.

b. That she typically uses her cellphone and iPad for accessing the internet.

c. That she is not familiar with programs such as Emule, peer to peer file

sharing, or Napster.

d. That her husband usually went to bed around midnight while she went to bed approximately 10:30-11:00 pm.

e. That the password for the desktop was "allen dale 1" and she also knew the passcode to her husband's cellphone.

f. That she does not know who their internet provider is because she does not pay the bills.

g. That she did not know what officers were referring to when they used the term "Alienware".

h. After officers explained that Alienware was the brand of desktop computer, KOSS's wife stated that they purchased the computer approximately 4 years ago and that it was new when they purchased it.

i. Officers also explained that there were files found on one of the computer at the residence that included the terms "PTHC" and "13YO". KOSS's wife did not recognize any of the names.

29. Based on my training and experience, I know that "PTHC" means "preteen hardcore" and "YO" refers to "years old", in this case "13YO" would refer to 13 years old.

30. The State of Oklahoma search and seizure warrant included the authority to forensically examine the devices seized from the residence. According to Lt.

Swafford's report, on December 2, 2019, the Alienware computer, item 18, was forensically examined and reviewed. Upon review of the contents, SPD Lt Swafford located 135 image files containing CSAM. SPD Lt. Swafford reported that some of the image files showed photographs of children engaged in sexual intercourse with adult males and then others showed children engaged in oral sex with other children under the age of 18 years of age.

31. Additionally, according to SPD Lt. Swafford's report, one of the 7 thumb drives recovered was forensically examined and reviewed. According to Lt. Swafford's report, 15 deleted videos containing CSAM were located on this thumb drive.

32. On November 30, 2023, items 1-18 and SPD reports were turned over by SPD to me for further investigation. The SPD reports only indicates reviews of the contents of the Alienware computer and one of the thumb drives. Both of the devices were reported to contain CSAM.

33. The hash values of the CSAM files that were discovered were submitted to NCMEC on January 17, 2020. The hash comparison resulted in 6 identified children. The following MD5 Hash values were flagged by NCMEC as containing identified children:

5b2ad73a4a08a2e35fe6d18734e63190
9ee2026bcc92cc1aca490798dacea753
1da31d8bcd1cab65251a9de47e369619
3656d18f9418eec6f154374446cfa55a
95e8202f72dfef4675030250b73e8118
2b94d1de307a84956d1838749411bd81

34. The SPD reports indicate that KOSS's Apple iPhone 7 was locked with a

complex passcode and that SPD was unable to get into the device. The reports do not indicate whether or not the other items listed in this warrant were reviewed.

35. KOSS is a member of the Cherokee Nation. Due to the *McGirt* decision, this investigation was transferred from the state of Oklahoma to the Northern District of Oklahoma for prosecution. This search warrant is being sought as a result of this decision to review the contents of the forensic images of the Devices. Should there be any errors when attempting to open the forensic images, this search warrant also requests to forensically retrieve the evidence stored within the Devices.

36. On January 2, 2024, OKDHS Assistant Special Agent in Charge contacted me regarding the Dell Laptop that was used by KOSS during his employment with OKDHS. During his interview KOSS admitted that while working at OKDHS, there was an allegation that he touched a 4 year old girl of a family he was assigned to.

37. Based on my training and experience, I know that individuals with a sexual interest in children often use multiple electronic storage devices to store their collection of CSAM. In this case, items 1-18 were located inside the residence where both KOSS and his wife lived and KOSS admitted to mostly maintaining control of the devices. Additionally, KOSS admitted to being familiar with the BitTorrent program, which is a peer-to-peer file sharing program that allows users to download and distribute digital files. Item 19 is KOSS's work laptop that was used by KOSS during his employment with OKDHS. KOSS was employed with OKDHS during the time the Oklahoma State search warrant was conducted.

38. Additionally, I know that individuals with a sexual interest in children will often download CSAM to one device and transfer the CSAM to other devices. Since KOSS had access to multiple devices and CSAM was found on at least two of those devices, it is possible that KOSS transferred CSAM from one device to another. Additionally, KOSS admitted to law enforcement that he was familiar with the BitTorrent file sharing program (a peer-to-peer file sharing program) and had used that program before.

39. The Devices are currently in the lawful possession of HSI. It came into the HSI's possession in the following way: the devices and extractions were turned over to me on November 30, 2023 from Sapulpa Police Department and on January 8, 2024 from OKDHS.

40. The Devices are currently in storage at 125 W 15th St. Tulsa, Oklahoma 74119. In my training and experience, I know that the Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of HSI.

Technical Terms

41. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data

communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This

storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using

specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be

used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

42. Based on my training, experience, and research, I know that the Devices have

capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, PDA, a tablet, and a device to access the internet utilizing an IP address. In my training and experience, examining data stored on devices of these type can uncover, among other things, evidence that reveals or suggests who possessed or used the Devices.

Characteristics Common to Individuals who Exhibit a Sexual Interest in Children and Individuals who Distribute, Receive, Possess and/or Access with Intent to View Child Pornography

43. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who distribute, receive, possess, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity;

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials

to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts;

c. Such individuals almost always possess and maintain digital or electronic files of child pornographic material, that is, their pictures, videos, photographs, correspondence, mailing lists, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, videos, photographs, correspondence, and mailing lists for many years;

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis;

e. Based on my training and experience and speaking with other special agents, I know that such individuals have taken their electronic devices and storage media, which contain their collections of child pornography, with them when they have moved or changed residences;

f. Such individuals may also take it upon themselves to create their own child pornography or child erotica images, videos or other recordings, or engage in contact sex offenses with children. These images, videos or other recordings may be taken or recorded covertly, such as with a hidden camera in a bathroom, or the individual may have child victims he or she is abusing in order to produce child pornographic or child erotica images, videos or other recordings. Studies have shown there is a high cooccurrence between those who traffic in child pornography and commit sex offenses with children. Such individuals may also attempt to persuade, induce, entice, or coerce child victims in person or via communication devices to self-produce and send them child pornography or to meet in person for sex acts. These images, videos or other recordings are often collected, traded, or shared;

g. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted"[1] it;

h. Such individuals also may correspond with and/or meet others to share

---

[1] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography;

i. Such individuals prefer not to be without their child pornography for any prolonged period of time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

Background on Child Pornography, Computers, and the Internet

j. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following: Computers, smartphones[2] and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers and smartphones basically serve four functions in connection with child pornography: production, communication, distribution, and storage;

k. Digital cameras and smartphones with cameras save photographs or videos as

---

[2] Smartphones are a class of mobile phones and of multi-purpose mobile computing devices. They are distinguished from feature phones by their stronger hardware capabilities and extensive mobile operating systems, which facilitate wider software, internet (including web browsing over mobile broadband), and multimedia functionality (including music, video, cameras, and gaming), alongside core phone functions such as voice calls and text messaging.

a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos;

l. Most portable digital devices contain SD cards (memory cards). Images can be saved to an SD card. An SD card with images saved on to it can be removed from one device and placed into a different device.

m. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers and smartphones and tablets around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone;

n. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are

plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also almost always carried on an individual's person (or within their immediate dominion and control) and can additionally store media;

o. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion;

p. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone or external media in most cases; and

q. As is the case with most digital technology, communications by way of computer or smartphone can be saved or stored on the computer or smartphone used for these purposes. Storing this information can be intentional (i.e., by

saving an e-mail as a file on the computer or smartphone, or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer or smartphone user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

Specifics of Search and Seizure of Computer Systems

44. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Devices in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media, such as a cellular phone, smartphone, or tablet. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

45. I submit that there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have

been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data;

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file;

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information;

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

46. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant but also for forensic electronic evidence that establishes how the Devices were used, the purpose of the use, who used the Devices, and when. There is probable cause to believe that this forensic electronic evidence will be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified;

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the

United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that logs the following: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular

location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement);

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when;

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored

on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant;

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent;

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

47. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that

computer data can be stored on a variety of computer systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, smartphones, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with

computer personnel who have specific expertise in the type of computer, software website, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of a premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the

data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

48. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

Electronic Storage and Forensic Analysis

49. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

50. I know that cellular telephones are often equipped with digital cameras and those phones possess the capability to transmit and/or store electronic images. I know that in many cases, cellular telephones maintain photographs of illegal activities, including possession, receipt, and distribution of CSAM. These photos are sometimes stored in their cellular phones and often are transmitted or sent from one electronic media device to another. I also know that cellular phones may also contain notes regarding potential illegal acts that are recorded by the subject who possesses the electronics. Furthermore, I know that text messages and emails are often used by two or more persons to communicate information regarding illegal activities, between principals and co-conspirators of those crimes.

51. I know that cellular telephones are utilized by the majority of individuals in the United States and have become a staple of communication between individuals using text messaging, visual and audible communications (telephone calls and FaceTime type communications) as well as applications like "Whatsapp" and "GroupMe." Additionally, individuals utilize their cellular devices to take pictures, keep notes, as a GPS (global positioning System) device, and even to conduct illicit or illegal activity. Communications on phones are kept for long periods and transferred from one phone to another when replaced. This is done through the use of Cloud storage and direct transfer conducted at the time of purchase or by the individual themselves. Individuals utilize this method as not to lose data that is stored on the phone such as contacts, photos, notes, and other important information

to the individual. This data includes contacts used to conduct illegal activities to include possession, receipt, and distribution of child pornography.

52. Cellular telephones are often used to facilitate offenses and allow criminals to maintain communication with each other before, during and after the commission of offenses. I am aware that cellular telephones have the capacity to store a vast amount of information, including but not limited to: telephone numbers, voice messages, text messages, e-mail, photographs, videos, address books, records, phone call histories, contact and other information. This information may be contained on the cellular telephone.

53. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to view, possess, and download CSAM, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe

that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

54. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

55. *Manner of execution*. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

56. *Methods of examination*. In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crimes under investigation, including but not limited to undertaking a cursory inspection of all information within the Devices. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information

subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications. Consequently, often many communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

Conclusion

57. Based on the information set forth in this affidavit, I submit there is probable cause to believe that Title 18 U.S.C. §§ 2252(a)(2) and (b)(1) (Receipt and Distribution of Child Pornography) and 18 U.S.C. §§ 2252(a)(4)(A) and (b)(2) (Possession of Child Pornography in Indian Country), have been violated, and that evidence of these offenses, more fully described in Attachment B, are located on the Devices described in Attachment A. I respectfully request that this Court issue a search warrant for the property described in Attachment A, authorizing the seizure of the items described in Attachment B.

58. Based upon my training and experience, I have learned that criminals who utilize the Internet actively search for criminal affidavits and search warrants and disseminate them to other criminals as they deem appropriate, i.e., post them publicly online through forums. It is possible that additional suspects will be discovered during forensic analysis of electronic devices. Premature disclosure of the

contents of this Affidavit and related documents may have a significant and negative impact on this continuing investigation and may jeopardize its effectiveness by alerting the potential target(s) to the existence and nature of the investigation, thereby giving them an opportunity to flee, or to destroy or tamper with evidence.

59. I request to be allowed to share this affidavit and the information obtained from this search with any government agency, to include state and local agencies investigating or aiding in the investigation of this case or related matters, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions from this matter.

Respectfully submitted,

Erin Staniech
Special Agent
Homeland Security Investigations

Subscribed and sworn to by phone on April 16, 2024.

SUSAN E. HUNTSMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

The property to be searched are as follows, hereinafter the "Devices":

1. Apple iPhone A1778 IMEI 358586092672637;
2. Samsung SM-G970u IMEI 352811101068728;
3. Samsung SGH-I337 IMEI 356567057346213;
4. Samsung SM-G891A IMEI 358518072719411;
5. Samsung SM-G850A IMEI 355956060549569;
6. Samsung SM-G930A IMEI 357425077311619;
7. 7 thumb drives;
8. 5 SD Cards;
9. SanDisk Ultra Plus 32 GB;
10. SanDisk Extreme Pro 32 GB;
11. Western Digital External Hard Drive;
12. Seagate External Hard Drive;
13. GB SanDisk card (found in a White Nikon Coolpix Camera);
14. Apple iPad 4;
15. ACER Laptop;
16. HP Laptop;
18. 18. Alienware Aurora R5 GTX1070; and
19. 19. Dell Laptop S/N 27807611078.

The Devices are currently located at 125 W 15th St. Tulsa, Oklahoma 74119.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

All records on the Devices described in Attachment A that relate to violations of Title 18 U.S.C. §§ 2252(a)(2) and (b)(1) (Receipt and Distribution of Child Pornography) and 18 U.S.C. §§ 2252(a)(4)(A) and (b)(2) (Possession of Child Pornography in Indian Country) involving Joseph KOSSs, including: Images/videos/gifs of child pornography or child erotica; files containing images/videos/gifs; and data of any type relating to the sexual exploitation of minors or a sexual interest in children, material related to the possession thereof, and data of any type related to any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting such visual depiction of such conduct, in any form wherever it may be stored or found, including, but not limited to:

i. Graphic Interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG) of child pornography; files relating to the distribution, receipt, or possession of child pornography, or information pertaining to an interest in child pornography;

ii. Files in any form containing the visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors; and

iii. Stories, text-based files, motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors.

A. Information, correspondence, records, documents or other materials pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to the sexual exploitation of minors or a sexual interest in children, that were transmitted or received using computer, cellular device, personal digital assistant, or some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

i. Correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children;

iii. Any and all electronic and/or digital records and/or documents pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States mail or by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256 or relating to the sexual exploitation of minors;

iv. Any and all electronic and/or digital records and/or documents including any and all address books, names, and lists of names and addresses of minors visually depicted while engaging in sexually explicit conduct, defined in Title 18, United States Code, Section 2256; or relating to the sexual exploitation of minors;

v. Any and all records of Internet usage including usernames and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums;

vi. Any physical keys, encryption devices, dongles and similar physical items necessary to access computer equipment, storage devices or data;

vii. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data; and

viii. Files, records, programs, logs, electronic communications, scanning programs, financial records, hacking software, or router configuration software.

B. Records or other items which evidence ownership, use, or control of the Devices described in Attachment A.

C. Credit card information including but not limited to bills and payment records, including but not limited to records of internet access.

D. Any and all information, correspondence (including emails), records, documents and/or other materials related to contacts, in whatever form, with minors involving the production, possession and/or distribution of child pornography and the attempt or act of educing, enticing, coercing, or persuading a minor to engage in sexual acts.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.